IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:	)	Group Art Unit:	2137
	)		
REISMAN	)	Examiner:	NGUYEN, M.
	)		
Serial No.: 09/435,736	)	Confirmation No.:	5609
	)		
Filed: November 8, 1999	)	PRE-APPEAL BRIEF REQUEST FOR REVIEW	
	)		
Atty. File No.: 4366-41	)		
	)		
For: "ENCRYPTED AND NON-ENCRYPTED COMMUNICATION OF MESSAGE DATA"	)		

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The outstanding Office Action rejects the claims under various combinations of Brendel, Johnson (6,529,885), Trcka, Gregg, Schneier and Johnson (5,923,885).

The Office Action further objects to claims 2-4, 6, 13, 16-18, 20, 23, 26, 30 and 34. Appellants agree with the Examiner's interpretation of these claims and for purposes of this Appeal would like those claims interpreted consistent with ¶ 7 of the Final Office Action.

Independent Claim 36 is directed toward a method of communication of data between a first computing device and a second computing device, comprising, *inter alia*, the program on the first computing device receiving a message from the user, wherein the message comprises at least a first and second datum input by the user into the at least first and second input fields, respectively, of the Web page, wherein the first datum is confidential to the user and the second datum is non-confidential to the user, and wherein the first datum comprises at least one of a credit card number and a social security number, the program identifying that the first datum is confidential and the second datum is non-confidential, the first computing device communicating, to the second computing device over an untrusted network, the first datum with encryption and first computing device communicating, to the second computing device over the

untrusted network, the second datum without encryption, wherein the communicating steps occur at least substantially simultaneously.

Independent Claim 40 is directed toward a comparable means, and Independent Claim 44 recites, *inter alia*, a program determining which of the at least first and second user input fields contains confidential information, wherein the first datum is confidential to the user and the second datum is not confidential to the user, the first computing device communicating the first datum to a second computing device over an untrusted network with encryption of the first datum and the first computing device communicating the second datum over the untrusted network to the second computing device without encryption of the second datum.

Independent Claim 45 recites, *inter alia*, a procedure operable to identify that the first datum is confidential and the second datum is non-confidential, wherein a second communication device is in communication with the first communication device and wherein the first computing device communicates, to the second computing device over the untrusted network, the first datum with encryption and the second datum without encryption.

As discussed in the specification, the entry (input) fields allow a user to input characters or text. These entry (input) fields are portions of a web page that can include, for example, a number of entry fields and a number of presentation fields. (See, for example, pgs. 7 and 8 of Appellants specification.)

Appellants respectfully submit the Office has failed to meet the minimum requirements to uphold *a prima facie* case of obviousness in that at least two features of the independent claims are neither taught nor suggested by any of the references of record.

First, the independent claims include either a program, means, or procedure that identifies that the first datum is confidential and the second datum is non-confidential. While the Office Action points to col. 11, lines 46-47, and col. 1, lines 37-42 of Brendel, Appellants respectfully submit there is absolutely no teaching or suggestion in these portions, nor any other portion of Brendel, that teaches the claimed feature. Specifically, the relied upon portion of col. 11 of Brendel merely states that "When the user is ready to check out, encrypted request 64 is sent by the client to the server farm." Col. 1 of Brendel states:

> The load on the server machine can be reduced by limiting the amount of data that is encrypted before being sent over the Internet. Less critical data such as product descriptions and advertisements can be sent as non-

encrypted data, while only the more critical data such as credit-card numbers are encrypted. The non-encrypted or clear-text data can be sent using standard or clear-text TCP/IP connections while the encrypted data is sent using an encrypted session.

Neither of these portions, nor any other portion, make any reference whatsoever to functionality nor componentry that is capable of performing the claimed feature.

Secondly, the independent claims are directed toward first and second input fields for input from the user.

The Office Action equates the first input field to the credit card in Brendel and the second input field to the purchased items of Brendel with reference to col. 10, lines 21-34.

The relied upon portion of Brendel states:

> FIG. 9 is an example of an atomic operation that assigns a server to a client for both clear-text and encrypted connections. A typical e-commerce web site provides clear-text web pages to users that show and describe products (catalog pages). The user can select a product for purchase by checking a check box or button on the product description page or a page with a list of products. Often the user continues to browse other products after a product has been selected for purchase. The selected product is put into a database maintained on the server, while the user continues to browse, perhaps adding other items to his "shopping cart."

While Brendel indicates that the user can select a product for purchase by checking a box or button on the product description page or a page with a list of products, Appellants respectfully submit this is not, and cannot under any reasonable interpretation be equated to the input fields as claimed.

Thus, Brendel lacks any teaching or suggestion of the first and second input/entry fields as claimed.

The fundamental operation of Brendel is also entirely different than that of the claimed invention. In Brendel, a common e-commerce configuration is described in which web pages containing one or more confidential fields are encrypted in their entireties while web pages not containing one or more confidential fields are not encrypted at all. Brendel does not teach or suggest that only flagged portions of web pages are encrypted while unflagged portions of the same web page are not encrypted, or vice versa.

Brendel does not disclose sending different information from different fields of a common Web page in two different forms, namely encrypted (for confidential information) and unencrypted (for non-confidential information).

In Johnson, SSL is used to encrypt all communications between the Web buyer and Web buyer's home bank so that *"electronic eavesdroppers between the Web buyer and the Web buyer's home bank cannot intercept any clear, unencrypted communication"* and the encryption used by the Web buyer's home bank's server to save the password is different from SSL and is applied locally *after* the password is received by the server and *not* before, as the Office asserts.

Johnson teaches what has always been done – namely, encryption of all, rather than selected, fields on the client's display during transmission to a server.

In that the remaining references, taken either alone or in combination, fail to overcome the deficiencies noted above, Appellants respectfully submit that a *prima facie* case of obviousness has not been established. Moreover, in that the cited references fail to teach or suggest the need to distinguish between confidential and non-confidential information in the same Web page, there is no incentive or motivation to use the applet distribution mechanism of Johnson in the architecture of Brendel to realize the claimed invention.

The dependent claims are even further patentably distinct from the cited art.

By way of example, claim 2 recites the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum to include the step of communicating the first datum with encryption and the second datum without encryption in a same packet that comprises the message. *See also* Claims 16, 37, and 42. This feature is neither suggested nor disclosed by the cited references.

Dependent claim 3 recites the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum to include the steps of communicating the first datum with encryption in a first packet of the message and communicating the second datum without encryption in a second packet of the message different from the first packet of the message. *See also* Claim 17. This feature is neither suggested nor disclosed by the cited references.

Dependent claim 4 recites the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum comprise the step of employing a same path between the first computing device and the second computing device to communicate the first datum with

encryption and the second datum without encryption. *See also* Claims 18, 38 and 43. This feature is neither suggested nor disclosed by the cited references.

Dependent claim 5 recites the step of employing the same path to communicate the first datum with encryption and the second datum without encryption to include the step of employing a TCP/IP passage between the first computing device and the second computing device to communicate the first datum with encryption and the second datum without encryption. *See also* Claim 19. This feature is neither suggested nor disclosed by the cited references.

Dependent claim 6 recites the step of communicating the first datum of the message with encryption of the first datum to include the step of employing a key to encrypt the first datum of the message for communication of the first datum from the first computing device to the second computing device with encryption of the first datum. *See also* Claims 7-9 and 20-22. This feature is neither suggested nor disclosed by the cited references .

Dependent claim 10 recites the Web page to include hypertext markup language, the first datum to include the credit card number, the second datum to include information related to a purchase by the user and the program to be embedded in the Web page. The program is loaded on the first computing device after the Web page is received by the first computing device. *See also* claims 33, 38, and 43. This feature is neither suggested nor disclosed by the cited references.

Remand of the case to the Examiner for a prompt Notice of Allowance is thus earnestly solicited.

The Notice of Appeal is believed to be timely and no additional fee is believed to be required. However, please credit any overpayment or debit any underpayment to Deposit Account 19-1970 and if an extension is required such extension is hereby petitioned.

Respectfully submitted,
SHERIDAN ROSS P.C.

By:_____
Jason H. Vick
Registration No. 45,285
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: 17 Nov. 11

J:\4366\-41\pre-appeal brief.wpd